International Journal of Control Theory and Applications

ISSN : 0974–5572

Volume 10 • Number 23 • 2017

Reinforcing Secure on-Demand Routing Protocol in Mobile AD-Hoc Network using Dual Cipher based Cryptography

K.Vinayakan[a] and M.V. Srinath[b]

[a]*Assistant Professor, Department of Computer Applications, STET Women's College, Mannargudi.*

[b]*Director, Department of Computer Applications, STET Women's College, Mannargudi.*

Abstract : Mobile ad-hoc network (MANET) lacks proper infrastructure and it is mostly Internet Protocol based network comprising of wireless points connected with radio. MANET are not centralized node of an administration mechanism. A Manet environment has to meet out certain inconsistencies arising out of limitation in their modus operandi. Many researchers have taken up the daunting task of studying the issues related to the MANET's and have devised various procedures to secure on-demand routing protocols in MANET's. However, many issues remain open in secure on-demand routing for MANET's. The main theme of this paper is to insinuate a new method for securing the on-demand routing protocol by employing a key generation technique which employs Dual Cipher Based Cryptography (DCBC). The route discovery procedure is also secured by employing Schnorr digital signature.

Keywords: *Ciphers, Multiple encryption, DNA based key Generation, Adhoc Network, Schnorr digital signature, Security.*

1. INTRODUCTION

1.1. Manet Network Routing Protocols and Attacks Related to it

The advancements in the computer age has bring more sophistication's in the day to day life of every individual. These advancements has influenced every aspect of computer science and has made the evolution in an enormous amount which never gave the humans the required time to take up and enjoy these advancements in it's true found state as the change was constantly happening. One such evolution is the advancement in MANET.[1] These networks always have routing as their core functionality and will usually have multi-hop transmissions before reaching the destination.

The Internet architecture as we know comprises of multiple domain spaces and the nodes present in these spaces use mobile IP technology as there is no single fixed domain space. As the part of fixed domain space is lacking in these infrastructures, the nodes are mostly in the roaming state. So the security aspects and the route discovery part of such nodes are dependent upon the routing protocol employed and the nature of the routing protocol is dependent upon the level of implementation of the protocol in the physical topology sense as the connection may be with a non native subnet or it can even be a wireless connection. So this lack

of physical infrastructure means there must be a more robust architecture where the subnet management and the harmonious working of the employed protocols are most needed. The main part is the routing functionality which is dependent upon the routing protocol that is previously engaged.[2] But the actual problem lies in the implementation of the routing part in the realm of autonomous wireless domains where the lack of fixed infrastructure makes the routing architecture difficult. In adhoc networks, the host which is a part of the network has to do two main functions namely the node part which is the sub part of the entire architecture and as the router which is the main functionality of the entire architecture. There is a lack of centralized control of packet transmission security here.

The concept of on demand routing requires more research and study as it has revolutionized the way of operation of most of the routing technologies. The on demand routing has its own detriments like network stagnation due to packet flooding and increased latency. The process of routing requires three agents viz the source, the destination and the routing table to validate the former and the latter. The chances of attack in the process of routing is high as the anonymous factors supporting various types of attacks can be found predominantly in any network environment with or without security consents. So when it comes to the factor of designing a routing protocol for Mobile Adhoc Network which is self contained and secure, we have to consider a lot of factors like maximum capacity of the medium of transmission, node characteristics and the topology of the network employed. When an attacker targets a Mobile ad-hoc Network, the attack is usually based on two things, the employment of the nodes and the functionality of the topology served. Various types of attacks on Routing which are mostly based on the techniques used and the consequences pertained due to the usage of those techniques is shown figure 1.

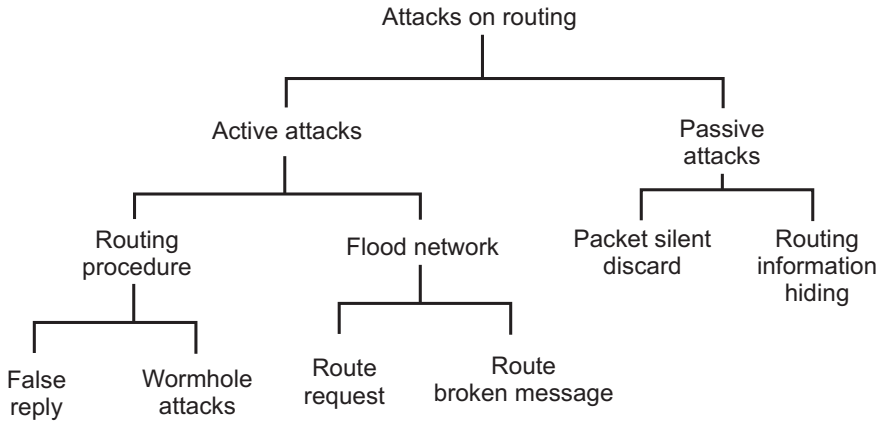

Figure 1: Various types of attacks on Routing

2. CORRELATED WORK

2.1. Cryptography

Cryptography is the method of concealing the actual message for the purpose of furtiveness. It includes mathematical techniques and models. In Cryptography, the plain text is converted to some arbitrary inconsequential text by adding cipher to it. This process is termed as encryption. Then that encrypted text is converted back to the plain text by removing the added cipher. This is known as decryption. This cipher which is occupied with the process of encryption and decryption can be a mathematical function or it can be a chunk of symbols which can be in fixed capacity or with continuous streams. The type of cipher used to encrypt and decrypt determines the level of security that is created as the cipher plays a very crucial role in the security process.

2.2. Attacks in Mobile Ad-hoc Networks

The proposed work actually insinuates a new method for securing the on-demand routing protocol. The main target for any attacker in a MANET is the Network layer where most of the core functionalities happen. The attacks that target the Network layer are segregated into two main tiers namely Active attacks and Passive attacks.[5]

In Active attacks, the attacker gain access to any participating node and will alter the transmitted data whose aftereffect will be network agitation. In Passive attacks, the attacker will never disturb the network rather the attacker tries to access any network prized assets which is consolidated by analyzing he network traffic. The main motivation of the attacker to carry out a network attack is to disrupt the network and bring down the services running in the network. The routing functionality of that network which is under attack can be assessed using various techniques.[19][20]The assessment results is always a condition where the infected node or the disrupted network model is inaccessible in whatever recovery technique. But if the routing model is modified to resurrect the infected node by means of any secure routing algorithm technique where the infected node is affected all together when choosing the nodes for transmission, the topology becomes stable again.

3. SYSTEM MODEL EXISTING SCHEME OF ROUTING PROTOCOLS IN MOBILE AD HOC NETWORKS

The current scheme of the routing protocols employed in the Mobile Ad-hoc networks use ciphers which are unvaryingly apportioned in the encrypting and the decrypting process. These ciphers are keys that are created based on the type of network topologies they are involved. The clusters involved in the communication share the same ciphers between them and the endorsement of validity is achieved through public-key cryptography.

In Mobile Ad-hoc Networks, most of the time there will be a common structure giving the authentication which will ensure that the communication happening over the network. In a typical Mobile Ad-hoc Network, there will be a Public Key Infrastructure (PKI) where the centralized authentication and authorization takes place. The Certificate Authority present in the Mobile Ad-hoc Networks is the primary agent of security without whose the security part is a big question mark in them as the Certificate Authority validates the nodes for authenticity.[14][15][16] This means that when a Certificate Authority present in the Public Key Infrastructure is compromised then that Mobile Ad-hoc Network is under compromising. The proposed procedure employs key generation using a novel method known as Dual Cipher Based Cryptography (DCBC). The authenticity of the route meant for destination is secured by employing Schnorr digital signature.

3.1. Proposed Security Mechanism for Manet

The propose method is very secure as it is a two way propagation of security techniques where the route integrity and the route discovery authenticity is maintained at its natural state.

3.1.1. Dual Cipher Based Cryptography (DCBC)

This method of Dual Cipher Based Cryptography is a novel method where the key is strengthen by adding more bits in a progressive manner where at step of the procedure the key is tighten by the attributes depending on the nodes employed in the topology rather than any third party authorization architecture which may be a threat of attack.[3][4][21] This kind of key generation technique is called as multiple encryption. In the process of multiple encryption, the intended message or the key(in our context) is encrypted more than once using the same process or by employing a different process. This process of super encipherment is carried out in a procedural way to prevent risk of key modification, either partly or completely.

3.1.2. Schnorr digital signature algorithm

Schnorr digital signature is used as the technique for securing the route discovery process in this process. Schnorr digital signature have stronger security proof when compared to other digital signatures.[6][7] Even though they are simple digital signatures, they can be implemented in a quick way with the possibility of creating more multi-signatures.

3.1.3. DNA based Key Generation

DNA contains the biological directives that make each species inimitable in the sense of uniqueness. The DNA is made up of nucleotides. There are primarily four types of nitrogen bases found in nucleotides. They are Adenine (A), Thymine (T), Guanine (G) and Cytosine (C). The progression or the pecking order, of these bases determines the biological directives that are confined in a strand of DNA. Each nucleotide is assigned a specific binary pair for identification as Adenine (A) for 00, Cytosine (C) for 01, Guanine (G) for 10, Thymine (T) for 11 respectively. The nucleotides are then given their respective DNA Key by a 2 bit addition process in which the first two bits are transposed and are added as their additional last two bits making them 4 bits as given in Table 1.

Table 1
DNA Key generation

Nucleotide	*bits*	*DNA Key*
Adenine (A)	00	0011
Cytosine (C)	01	0110
Guanine (G)	10	1001
Thymine (T)	11	1100

3.1.4. Dual Cipher Based Cryptography Key Generation process

This is a novel method in which the key generation part is made manually with no mathematical models and yet powerful when it comes to encryption and decryption. The key generation is the main aspect of any cryptographic transmission.[8][9][22] The process of generating the keys and the methods of preserving and managing the generated keys is vital part. This process of Key generation is a Three step procedure.

Step 1: The participating nodes are assigned a new 4 digit number known as Participating Node Identification number (PNID). This PNID is based on a few attributes of the participating nodes like the CPU capability, memory employed and power storage. Every digit has its own implication

First digit: CPU capability for the network

0 : Less CPU

1 : Optimal CPU

Second digit: Memory employed

0 : Average Memory capacity

1 : Optimal Memory capacity

Third digit: Power storage

0 : Energy storage nodes

1 : Energy harvesting nodes

Fourth digit: Node transmission Speed

0 : Transmission speed below 1000Mbps

1 : Transmission speed above 1000Mbps

For example, a node with an optimal memory and CPU capacity but has an energy harvesting capability with the transmission speed below 1000Mbps will be given a PNID of 1110.

Step 2: The MAC address of each node is added with the PNID to generate a Immediate Encryption Key (IEK).

MAC address(48 bits) + PNID (4 bits) = IEK (52 bits)

Step 3: The 52 bits of Immediate Encryption Key (IEK) is compared with the DNA based Key Generation technique and a new DNA based Immediate Encryption Key (DIEK) is generated which is 104 bits in length.

Step 4: The generated DNA based Immediate Encryption Key (DIEK) which is 104 bits in length is converted to Dual Cipher Based Cryptography Key (DCBC key) 0f 128 bits by adding a 24 bit key which is generated by adding the Device ID part of the employed node's MAC address at the prefix of the DNA based Immediate Encryption Key (DIEK). The usage of Device ID part of the MAC address makes this encryption schema very unique as the key generated is 128 bits.

Sample execution of four steps in the Dual Cipher Based Cryptography Key generation:

Step 1: Node's PNID : 1110

Step 2: Node's MAC : 001D602F4B39

MAC address in Binary Format :

OUI part: 0000 0000 0001 1101 0110 0000

Device ID part: 0010 1111 0100 1011 0011 1001

Node's IEK : 0000 0000 0001 1101 0110 0000 0010 1111 0100 1011 0011 1001 1110

Step 3: Conversion of IEK to DNA base bits : AA AA AC TC CG AA AG TT CA GT AT GC TG

Conversion of DNA base bits to DNA based Immediate Encryption Key (DIEK): 00110011 00110011 00110110 11000110 01101001 00110011 00111001 11001100 01100011 10011100 00111100 10010110 11001001.

Step 4: Conversion of DIEK to Dual Cipher Based Cryptography Key (DCBC key):

Device ID prefix + DIEK = Dual Cipher Based Cryptography Key (DCBC key) [128 bits]

0010 1111 0100 1011 0011 1001 00110011 00110011 00110110 11000110 01101001 00110011 00111001 11001100 01100011 10011100 00111100 10010110 11001001

Encryption Process:

1. Assign Participating Node Identification number (PNID) to the node.
2. Convert the PNID to Immediate Encryption Key (IEK).
3. Convert the 52 bits of Immediate Encryption Key (IEK) to DNA based Immediate Encryption Key (DIEK).
4. Convert the DIEK to Dual Cipher Based Cryptography Key (DCBC key).

Decryption Process:

1. Device ID prefix is removed from Dual Cipher Based Cryptography Key (DCBC key) to get DNA based Immediate Encryption Key (DIEK).
2. DNA base bits are removed from the DIEK to get Immediate Encryption Key (IEK).
3. The MAC address is removed from the IEK to get the PNID of the respective nodes.

3.1.5. Fortified Route Discovery

In a Mobile Ad-hoc Network, when the source and the destination of a packet delivery is determined by the protocol, the efficiency of the available routes are taken into account.[10][11] But the security aspect is not considered as it requires more perspectives of the topology to be considered. But in reality, this lack of considerations of security procedures by the employed routing protocol poses as a greater threat model. [12][13][23]In the proposed scheme of process after the Dual Cipher Based Cryptography Key generation, the nodes will be ready to participate in the routing process.

When the process of routing starts, the source node is authenticated by using Schnorr digital signature. [17][18] The main hindrance is the verification part where the harnessed digital signature created by the source dispatcher can be corroborated with either the predestined receiver or the entire adherents of the Mobile Ad-hoc Network.

Schnorr signature scheme comprises of a series of mathematical directions that conjugates the private key, public key and signature together. The digital signature uses the Dual Cipher Based Cryptography key as the main key and the transacted data as the encipherment message.

4. CONCLUSION AND FUTURE WORK

In this paper we suggest a scheme which provides key generation by using Dual Cipher Based Cryptography (DCBC) as well as ensures secure route discovery by employing Schnorr digital signature in wireless ad hoc network. In order to strengthen the proposed scheme, the following challenges need to address in the future works: Redesign the protocol which can address multiple server groups in large partitioned networks and Redesign the scheme which can address multiple group node addition inclusive of node mobility.

REFERENCES

[1] Z.J.Haas, J.Deng, B.Liang, P.Papadimitratos, and S.Sajama. Encyclopedia of Telecommunications, chapter Wireless Ad Hoc Networks. John Wiley, 2002.

[2] Web page. Mobile Ad-hoc Networks (MANET) charter.http://www.ietf.org/html.charters/manet charter.html.

[3] “Multiple encryption” in “Ritter’s Crypto Glossary and Dictionary of Technical Cryptography”

[4] M. Maurer and J. L. Massey, Cascade ciphers: The importance of being first, Journal of Cryptology.

[5] Applied Cryptography, Second Edition: Protocols, Algorithms, and Source Code in C by Bruce Schneier. Wiley Computer Publishing, John Wiley & Sons, Inc.

[6] Bernstein, Daniel J., et al. “High-speed high-security signatures”. September 2011. http://ed25519.cr.yp.to/ed25519-20110926.pdf.

[7] Bernstein, Daniel J., et al. “TweetNaCl: A crypto library in 100 tweets “. September 2014. http://tweetnacl.cr.yp.to/tweetnacl-20140917.pdf.

[8] Dr. S. S. Tyagi and Aarti: Study of MANET: Characteristics, Challenges, Application and Security Attacks, International Journal of Advanced Research in Computer Science and Software Engineering

[9] Humayun Bakht, “ Survey of Routing Protocols for Mobile Ad-hoc Network”, International Journal of Information and Communication Technology Research

[10] Abdalla M, An J, Bellare M, Namprempre C (2002) Knudsen L (ed) Advances in cryptology- EuroCrypt 2004.

[11] Menezes AJ, van Oorschot PC, Vanstone SA (1997) Handbook of applied cryptography. CRC Press, Boca Raton

[12] A. Menezes, P. Van Oorschot and S. Vanstone,

[13] Handbook of Applied Cryptography , CRC Press, 1996.

[14] Stathis Zachos, Computational Number Theory and Cryptography, National Technical University Of Athens, 2012.

[15] Ç. Erdal and R. Chunming, Security in Wireless Ad Hoc and Sensor Networks, 1st ed , A John Wiley and Sons, Ltd, Publication, United Kingdom, 2009.

[16] Seyed Amin Hosseini Seno, Rahmat Budiarto andTat-CheeWan, 2011. A Secure Mobile Ad hoc Network Based on Distributed Certificate Authority, In King Fahd University of Petroleum and Minerals.

[17] Z. Ye, S.V. Krishnamurthy, S.K. Tripathi, A framework for reliable routing in mobile ad hoc networks, in: IEEE INFOCOM, San Francisco, CA, USA, 2003.

[18] Eastom, C. (2012). Computer Security Fundamentals (2nd Edition ed.). indiana: Pearson.

[19] Forouzan, B. A. (2007). Data Communications and Networking (4th Edition ed.). New York: McGraw-Hill.

[20] F. Fischer, J. Fuchs, P.-A. Vervier, F. Mansmann, and O. Thonnard, "VisTracer: A Visual Analytics Tool to Investigate Routing Anomalies in Traceroutes," in Proceedings of the Ninth International Symposium on Visualization for Cyber Security, ser. VizSec '12. New York, NY, USA: ACM, 2012.

[21] X. Luo, Y. Liu, J. Su and R. K. Chang, "Characterizing inter-domain rerouting by betweenness centrality after disruptive events," Selected Areas in Communications, IEEE Journal on, vol. 31.

[22] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," IEEE Trans. Inf. Theory, vol. 54, no. 6, pp. 2515–2534, Jun. 2008.

[23] J. Baek, R. Safavi-Naini, and W. Susilo, "On the integration of public key data encryption and public key encryption with keyword search," in Information Security ISC, 2006.

[24] B. Pinkas, T. Schneider, N. Smart, and S. Williams. Secure two-party computation is practical. In ASIACRYPT, 2009.